

FRANKEL et al. — 09/492,534
Client/Matter: 061047-0265649

IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Original) In an infrastructure in which some of a plurality of entities provide cryptographically supported services, a method of registering a subscriber entity of a plurality of entities at a principal entity of a plurality of entities, the method comprising:

the subscriber entity requesting service from the principal entity by sending a request message to a registrar entity of the plurality of entities;

the registrar entity verifying the subscriber entity and forwarding the request for service to the principal entity;

the principal entity storing the forwarded request and transmitting an acknowledgement message to the registrar entity, the acknowledgement stating acceptance and authentication/authorization information that the subscriber entity requires for the requested service; and

the registrar entity verifying the authenticity of the received acknowledgement message, and, if correct, forwarding the acknowledgement message to the subscriber entity.

2. (Original) A method as in claim 1 wherein the request message contains an indication of the type of service requested by the subscriber entity.

3. (Currently amended) A method as in claim 2 wherein the request message contains one or more of the following:

(a) a unique reference to the subscriber entity;

(b) attributes about the subscriber entity;

(c) authentication information to be used to authenticate use of the service;

(d) transactional verification information;

(e) a representation ~~representations~~ by the subscriber entity agreeing to what the entity subscriber accepts;

(f) a preferred service relationships ~~relationship~~; and

(g) a subscriber's subscriber entity's authenticator.

FRANKEL et al. -- 09/492,534
Client/Matter: 061047-0265649

4. (Currently amended) A method as in claim 3 wherein the unique reference to the subscriber entity is at least one of (a) the subscriber ~~subscriber's~~ entity's identity, (b) a pseudonym for one-time service, and (c) a pseudonym for continued use of the service
5. (Currently amended) A method as in claim 3 wherein ~~the~~ a session identifier links future responses to this particular request.
6. (Currently amended) A method as in claim 3 wherein the attributes about the subscriber entity include:
 - (a) a self-representations representation; and
 - (b) a third-party representation ~~representations~~ asserting attributes.
7. (Currently amended) A method as in claim 6 wherein said representation ~~representations~~ and attribute ~~attributes~~ include at least some of:
 - (a) an address ~~addresses~~;
 - (b) employment information;
 - (c) information from one or more other entities needed for service provisioning; and
 - (d) an authorization ~~authorizations~~ from another ~~other~~ party ~~parties~~.
8. (Original) A method as in claim 1 further comprising:
modifying the registration of the subscriber entity at the principal entity.
9. (Original) A method as in claim 1 further comprising:
moving the registration for service from the principal entity to another entity of said plurality of entities.
10. (Currently amended) A method as in claim 1 wherein the service includes:
operating a cryptographically-supported transaction involving the subscriber entity, the principal entity and possibly one or more additional entities.
11. (Original) A method as in claim 1 wherein the subscriber entity comprises a plurality of elements.

FRANKEL et al. — 09/492,534
Client/Matter: 061047-0265649

12. (Original) A method as in claim 11 wherein the plurality of elements are associated with an entity.
13. (Currently amended) A method as in claim 1 ~~wherein~~ ~~where~~ said service is a subset of a totality of services.
14. (Currently amended) A method as in claim 1 wherein said ~~where~~ service is a warranty service.
15. (Currently amended) A method as in claim 13 wherein another subset of the totality of services to the subscriber entity is provided by an entity different from the principal entity.
16. (Original) A method as in claim 15 wherein the subscriber entity can modify the subset of totality of services between entities.
17. (Currently amended) A method as in claim 8 ~~wherein~~ ~~where~~ modification is supervised by one or more authorities.
18. (Currently amended) A method as in claim 9 ~~wherein~~ ~~where~~ moving of services is supervised by one or more authorities.
19. (Currently amended) A method as in claim 1 ~~wherein~~ ~~where~~ provision of service may involve an additional entity from ~~the~~ said plurality of entities.
20. (Currently amended) A method as in claim 19 ~~wherein~~ ~~where~~ provision of service is split between said principal entity and said additional entity.
21. (Original) A method as in claim 1 wherein provision of service by said principal entity on behalf of said subscriber entity is given by said operating infrastructure to an entity within said plurality of entities.
22. (Original) A method as in claim 1 wherein said provision of service by said principal entity involves other entities within said plurality of entities.

FRANKEL et al. - 09/492,534
Client/Matter: 061047-0265649

23. (Original) A method as in claim 14 wherein said warranty service involves correctness of representation of information.

24. (Currently amended) A method as in claim 23 wherein said representation of information is at least one of: (a) identity information, (b) financial information; and (c) information derived from provision of service within said infrastructure.

25. (Currently amended) A method as in claim 14 wherein the ~~system~~ infrastructure includes a mechanism to initiate claims against failed warranty.

26. (Currently amended) A method as in claim 1 wherein ~~said service provision of service involve~~ involves control of access.

27. (Original) A method as in claim 1 wherein at least one of said plurality of entities is an enterprise.

28. (Original) A method as in claim 1 wherein at least one of said plurality of entities is a financial institute.

29. (Original) A method as in claim 1 wherein said principal entity is a group of elementary entities.

30. (Currently amended) A method as in claim 1 wherein ~~said~~ provision of service by said principal entity is directed by said subscriber entity.

31. (Original) A method as in claim 8 wherein registration modification transactions involve managing capabilities.

32. (Original) A method as in claim 8 wherein registration modification transactions involve cryptographic key management.

33. (Original) A method as in claim 1 further comprising:

FRANKEL et al - 09/492,534
Client/Matter: 061047-0265649

providing, by the principal entity, at least one of a set of various service transactions to the subscriber entity.

34. (Original) A method as in claim 33 wherein said providing involves the certification of digital identities.

35. (Original) A method as in claim 33 wherein at least one of said service transactions involves assuring an entity's state.

36. (Original) A method as in claim 33 wherein at least one of said service transactions involves assuring financial information.

37. (Original) A method as in claim 33 wherein at least one of said service transactions involves assurance of identity and assurance of entity's state.

38. (Currently amended) A method as in claim 1 wherein ~~where~~ some of said plurality of entities are supervised by one or more other entities in at least one transaction.

39. (Currently amended) A method as in claim 1 [[.]] wherein ~~where~~ service services involves involve a fee fees based on a service agreement agreements and contract contracts.

40. (Currently amended) A method as in claim 1 [[.]] wherein added ~~control management~~ and one or more additional entities assure integrity of transactions within the system infrastructure.

41. (Currently amended) A method as in claim 40 wherein ~~the~~ integrity of the management function is enhanced by providing two or more independent reports.

42. (Original) A method as in claim 40 wherein the management function controls actions of assurance offering entities on a per transaction basis.